

# [Albania]

# Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

## **Table of contents**

Version [24.03.2020]

[reference to the provisions of the Budapest Convention]

### **Chapter I – Use of terms**

Article 1 - "Computer system", "computer data", "service provider", "traffic data"

### Chapter II - Measures to be taken at the national level

Section 1 - Substantive criminal law

Article 2 – Illegal access

Article 3 - Illegal interception

Article 4 – Data interference

Article 5 - System interference

Article 6 - Misuse of devices

Article 7 - Computer-related forgery

Article 8 - Computer-related fraud

Article 9 – Offences related to child pornography

Article 10 - Offences related to infringements of copyright and related rights

Article 11 - Attempt and aiding or abetting

Article 12 - Corporate liability

Article 13 - Sanctions and measures

Section 2 - Procedural law

Article 14 - Scope of procedural provisions

Article 15 - Conditions and safeguards

Article 16 – Expedited preservation of stored computer data

Article 17 - Expedited preservation and partial disclosure of traffic data

Article 18 - Production order

Article 19 – Search and seizure of stored computer data

Article 20 - Real-time collection of traffic data

Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

### Chapter III - International co-operation

Article 24 – Extradition

Article 25 - General principles relating to mutual assistance

Article 26 – Spontaneous information

Article 27 – Procedures pertaining to mutual assistance requests in the

absence of applicable international agreements

Article 28 – Confidentiality and limitation on use

Article 29 – Expedited preservation of stored computer data

Article 30 - Expedited disclosure of preserved traffic data

Article 31 – Mutual assistance regarding accessing of stored computer

data

Article 32 – Trans-border access to stored computer data with consent or

where publicly available

Article 33 - Mutual assistance in the real-time collection of traffic data

Article 34 – Mutual assistance regarding the interception of content data

Article 35 – 24/7 Network

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.



State:	
Signature of the Budapest Convention:	22/11/2001
Ratification/accession:	19/06/2002

DOMESTIC LEGISLATION

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

#### **DOMESTIC LEGISLATION**

### Article 2 - Illegal access

necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer punishable by fine or imprisonment up to three years. system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

### Article 192/b - Illegal computer access

Each Party shall adopt such legislative and other measures as may be Unauthorized access or access in excess of the authorization to access a computer system or in a part thereof, through violation of the security measures, is

> When this very act is committed in military, national security, public order, civil protection, health computer systems or any other computer system of public importance, it is punishable by imprisonment from three up to ten years.

### Article 3 - Illegal interception

necessary to establish as criminal offences under its domestic law, when means, of non-public transmissions of computer data to, from or within a imprisonment committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

### Article 293/a - Illegal interception of computer data

Each Party shall adopt such legislative and other measures as may be The illegal interception, with technical devices, of the non-public transmissions of computer data from or within a computer system, including electromagnetic committed intentionally, the interception without right, made by technical emissions from another computer system carrying such data, is punished with an of three sentence to seven years. computer system, including electromagnetic emissions from a computer When this offence is committed from/within the computer systems of the system carrying such computer data. A Party may require that the offence be military, public order, civil protection or any other computer system of public importance, it is punished with an imprisonment sentence of seven to fifteen years.

#### Article 4 - Data interference

- necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- 2 A Party may reserve the right to require that the conduct described in punished with an imprisonment sentence of three to ten years. paragraph 1 result in serious harm.

### Article 293/b - Data interference

1 Each Party shall adopt such legislative and other measures as may be The damaging, deletion, alternation or unauthorized suppression of computer data is punished by an imprisonment sentence of six months to three years. When this offence is committed against the computer data of the military, public order, civil protection, health care or any other computer data of public importance, it is

### Article 5 - System interference

necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning punished with an imprisonment sentence of three to seven years. of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data

### Article 293/c - Interference in the computer systems

Each Party shall adopt such legislative and other measures as may be The serious and unauthorized hindering of the functioning of a computer system by inputting, damaging, deforming, altering, deleting or suppressing of data is

When this offence is committed in the computer systems of the military, national security, public order, civil protection, health care or any other computer system of public importance, it is punished with an imprisonment sentence of five to fifteen years.

### Article 6 - Misuse of devices

### Article 293/c - Misuse of devices

### **DOMESTIC LEGISLATION**

- committed intentionally and without right:
- a the production, sale, procurement for use, import, distribution or otherwise making available of:
- a device, including a computer program, designed or adapted primarily an imprisonment sentence of six months to five years.". for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
- a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
- the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
- 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
- 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

1 Each Party shall adopt such legislative and other measures as may be The production, possession, selling, procurement for use, distribution or otherwise necessary to establish as criminal offences under its domestic law, when making available of a device, including a computer programme, a computer password, access code or other similar data, designed or adjusted to access the whole or part of the computer system, for the purpose of committing the offences established in articles 192/b, 293/a, 293/b e 293/c of this code, are punished with

### Title 2 - Computer-related offences

### Article 7 - Computer-related forgery

necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent imprisonment that it be considered or acted upon for legal purposes as if it were authentic, When this act is committed by the person in charge of retaining and administering

### Article 186/a - Computer related forgery

Each Party shall adopt such legislative and other measures as may be Any input, alteration, deletion or suppression of data, without right, with the intent of creating inauthentic data, to be used and presented as authentic, regardless whether or not the data is directly readable or intelligible are sentenced with period months vears.

#### **DOMESTIC LEGISLATION**

regardless whether or not the data is directly readable and intelligible. A Party computer data, in cooperation, more than one time or when it has led to grave may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

consequences to the public interest, it is sentenced with imprisonment from three to ten years.

### Article 8 - Computer-related fraud

## necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- any input, alteration, deletion or suppression of computer data;
- b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic (five million) leke. benefit for oneself or for another person.

### Article 143/b - Computer fraud

Each Party shall adopt such legislative and other measures as may be Any input, alteration, deletion or suppression of computer data or interferences with the functioning of a computer system, with the fraudulent intent of procuring, without right, an economic benefit for oneself or of causing a loss of property to another person, are punished by an imprisonment sentence of six months to six years, and a fine of 60 000 (sixty thousand) leke to 600 000 (six hundred) leke. The same offence, when committed in cooperation, when causing damage to a number of persons, when committed more than one time, and when it has led to serious material consequences is sentenced with five to fifteen years of imprisonment and a fine of 500 000 (five hundred thousand) lekë to 5 000 000

### Title 3 - Content-related offences

### Article 9 - Offences related to child pornography

- necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
  - producing child pornography for the purpose of its distribution through a computer system;
  - offering or making available child pornography through a computer system;
  - distributing or transmitting child pornography through a computer system;
  - procuring child pornography through a computer system for oneself or for another person:
  - possessing child pornography in a computer system or on a computer-data storage medium.
- 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
  - a minor engaged in sexually explicit conduct;

### Article 117 - Pornography

1 Each Party shall adopt such legislative and other measures as may be Production, distribution, advertisement, export, import, sale, and publication of pornographic materials in environments with children, by any means or form, shall constitute criminal contravention and shall be punishable by imprisonment of up to two years.

> The use of minors for the purpose of producing pornographic materials, their distribution and publication in the internet or through other forms, is sentenced with imprisonment of five years and a fine of one million to five million leks.

#### **DOMESTIC LEGISLATION**

- a person appearing to be a minor engaged in sexually explicit conduct;
- realistic images representing a minor engaged in sexually explicit conduct
- 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower agelimit, which shall be not less than 16 years.
- 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

### Title 4 - Offences related to infringements of copyright and related rights

### Article 10 - Offences related to infringements of copyright and related Art.148, Art.149 of the Criminal Code of the Republic of Albania Art.14, Art.50 of riahts

- Each Party shall adopt such legislative and other measures as may be Art. 148 of the Criminal Code refers to Publication in someone's own name of necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to Art. 149 CC - Unlawful reproduction of someone else's work. the obligations it has undertaken under the Paris Act of 24 July 1971 revising Art. 14 of Law on copyright - free use of computer programs. such conventions, where such acts are committed wilfully, on a commercial the moral and economic rights of the author are violated. scale and by means of a computer system.
- Each Party shall adopt such legislative and other measures as may be ownership may include also the use of computer systems. necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
- A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other

the Law on Copyright.

the work of another person.

the Bern Convention for the Protection of Literary and Artistic Works, the Art. 50 of Law on copyright - violations or transmission in any hall or with any Agreement on Trade-Related Aspects of Intellectual Property Rights and the other means of artistic ownership, without permission, violating the dispositions WIPO Copyright Treaty, with the exception of any moral rights conferred by of this law or international agreements ratified by the Republic of Albania, when

The term "transmission in any hall or with any other means" of artistic

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary	liability and sanctions
Convention with intent that such offence be committed.  2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established	Considering the stage until the realization of the consequence, as well as the causes due to which the offence remained an attempt, the court may mitigate the sentence, and may lower it under the minimum provided for by law, or may decide for a kind of punishment milder than the one provided for by law.  Article 27 Criminal Code - Responsibility of collaborators Organizers, instigators, and helpers bear the same responsibility as the executors for the criminal act
Article 12 – Corporate liability  1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:  a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person.  2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.  3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.	Law nr.9754, dated 14.6.2007 "Criminal Liability for legal entity"

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
Article 13 – Sanctions and measures  1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.  2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	Art.117 Art.122, Art.123, Art.165, Art.186, Art.187, Art.188, Art.189, Art.190, Art.191, Art.192, Art.255, Art.286/a of the Criminal Code of the Republic of Albania.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions  1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.  2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:  a the criminal offences established in accordance with Articles 2 through 11 of this Convention;  b other criminal offences committed by means of a computer system; and  c the collection of evidence in electronic form of a criminal offence.  3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.  b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:	

#### **DOMESTIC LEGISLATION**

- i is being operated for the benefit of a closed group of users, and
- ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21

### Article 15 - Conditions and safeguards

- 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
- 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
- 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

#### Article 221 CPC - Limits of permission

- 1. The interception of conversations or telephone communication or other forms of telecommunication is permitted only when it is proceeded for:
  - intentional crimes punishable by imprisonment not less than five years maximum
  - crimes connected with arms or explosive matters, narcotic substances and contraband
  - criminal offences of insult and threat by phone call.

### Article 222 CPC - The decision permitting the interception

- 1. The court authorises the interception upon request of prosecutor or injured accuser, by motivated decision for cases permitted by law and when it is indispensable for the continuation of investigations, and when there exist enough facts to prove the accuse. The decision of the court, which refuses the request for interception, can be appealed.
- 2. When there are grounded reasons to think that the delay may bring serious damage to the investigations, the prosecutor orders the interception by a motivated act and informs the court immediately, but not later than twenty-four hours. The judge, within twenty-four hours from the order of the prosecutor, makes the evaluation by a reasonable decision. In case this is not made within the fixed time- limit, the interception cannot continue and its results cannot be used.
- The order for interception explains the way it shall be done and the timelimits, which cannot exceed fifteen days. The court may prolong this timelimit again to another fifteen days.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 16 – Expedited preservation of stored computer data  1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the	<u> </u>
expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable	data may be lost, damaged or altered.
to loss or modification.  2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may	
	1 '
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the	Article 101 "Preservation and administration of data for the purpose of
computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.	
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	<ul> <li>2 These records should contain data that enable:</li> <li>The identification of subscribers ensuring the registration of their full identity</li> <li>The identification of the end equipment used in the communication</li> <li>the identification of the date, hour, duration of communication and the number called</li> </ul>
	3. These records should be made available, also in an electronic form, to the authorities referred to in the Criminal Procedure Code, based upon their request.

#### **DOMESTIC LEGISLATION**

### Article 17 - Expedited preservation and partial disclosure of traffic Article 299/b - Expedited preservation and partial disclosure of computer data

Article 16, such legislative and other measures as may be necessary to:

- transmission of that communication; and
- ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under | The person in charge of expeditious preservation and maintain ace of the traffic data is obliged to undertake all the necessary measures to ensure that the stored ensure that such expeditious preservation of traffic data is available data is valid, regardless of whether one or more service providers were involved regardless of whether one or more service providers were involved in the in the transmission of the communication as well as to provide the prosecutor or the authorized judicial police officer with a sufficient amount of traffic data to enable the identification of the service provider and the path through which the communication was transmitted.

#### Article 18 - Production order

necessary to empower its competent authorities to order:

- person's possession or control, which is stored in a computer system or a computer-data storage medium; and
- submit subscriber information relating to such services in that service provider's possession or control.
- Articles 14 and 15.
- 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is hours after the notification. held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
  - the type of communication service used, the technical provisions taken thereto and the period of service;
  - the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

### Article 191/a - Obligation to produce computer data

- 1 Each Party shall adopt such legislative and other measures as may be 1 In the cases of proceedings related to criminal offences in the area of information technology, the Court, upon a request from the prosecutor or the a person in its territory to submit specified computer data in that plaintiff, orders a person to submit computer data in his possession or control, which is stored in a computer system or other data storage devices.
  - a service provider offering its services in the territory of the Party to 2 In these proceedings, the Court orders the service provider to submit all subscriber information relating to the services offered by the service provider.
- 3 When there are grounded reasons to believe that delays would seriously damage 2 The powers and procedures referred to in this article shall be subject to the investigations, the prosecutor, by means of a reasoned act, orders the production of computer data specified in points 1 and 2 of this article and notifies the court immediately. The Court reviews the decision of the prosecutor within 48

#### **DOMESTIC LEGISLATION**

any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

### Article 19 - Search and seizure of stored computer data

- necessary to empower its competent authorities to search or similarly access:
- a computer system or part of it and computer data stored therein; and
- b stored

in its territory.

- necessary to ensure that where its authorities search or similarly access a grounds to believe that the data sought is stored in another computer system | system as well. or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously 3 For the purpose of executing the court order, the prosecution or the judicial extend the search or similar accessing to the other system.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- seize or similarly secure a computer system or part of it or a computer-data storage medium;
  - make and retain a copy of those computer data;
  - maintain the integrity of the relevant stored computer data;
  - computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

### Article 208/a - Seizure of computer data

- 1 Each Party shall adopt such legislative and other measures as may be 1 In the cases of proceedings related to criminal offences in the area of information technology, the Court, upon a request from the prosecutor, orders the seizure of the data and the computer systems. The court specifies in the order the right to access, search and obtain data in a computer system, as well as the a computer-data storage medium in which computer data may be prohibition of further actions or the securing of the data or computer systems.
- 2 When there are reasonable grounds to believe that the computer data sought 2 Each Party shall adopt such legislative and other measures as may be is stored in another computer system or part of it, and that such data is legally accessible from or available to the initial system sought, the court, upon a request specific computer system or part of it, pursuant to paragraph 1.a, and have from the prosecutor, immediately orders the search or access to this computer
  - police officer delegated by the prosecutor takes measures:
    - To stop further activities or to secure a computer system or part of it and other data storage devices;
    - Make and retain copies of the computer data;
    - To render inaccessible or to remove those computer data from the accessible computer systems;
    - Maintain the integrity of the respective stored data.

render inaccessible or remove those computer data in the accessed | 4 In order to have these measures applied, the prosecutor may order an expert, who has knowledge about the functioning of computer systems or measures to be taken to protect the computer data therein. The designated expert cannot refuse the task unless he provides reasonable.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 20 – Real-time collection of traffic data  1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:  a collect or record through the application of technical means on the territory of that Party, and  b compel a service provider, within its existing technical capability:  i to collect or record through the application of technical means on the territory of that Party; or  ii to co-operate and assist the competent authorities in the collection or recording of,  traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.  2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.  3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.  4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data  1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:  a collect or record through the application of technical means on the territory of that Party, and  b compel a service provider, within its existing technical capability:  ito collect or record through the application of technical means on the territory of that Party, or	Articles 221-222 of Criminal Procedure Code provides for interception of conversations or telephone communication or other forms of telecommunication

### **DOMESTIC LEGISLATION**

ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its 1. In the general authorization AKEP may include conditions related to: territory transmitted by means of a computer system.

- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

#### **Article 15.- General Conditions**

f) permission for interception by competent authorities defined in the legislation

in force on interception of telecommunications and implementation of other liabilities arising out of this legislation.

#### Section 3 - Jurisdiction

#### Article 22 - Jurisdiction

- Each Party shall adopt such legislative and other measures as may be | Criminal Procedure Code Article 69, 73 necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
  - in its territory; or а
  - on board a ship flying the flag of that Party; or
  - on board an aircraft registered under the laws of that Party; or
  - by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
- Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
- This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

Criminal Code Article 7/a universal jurisdiction

#### **DOMESTIC LEGISLATION**

When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

### **Chapter III – International co-operation**

#### Article 24 - Extradition

- 1 a This article applies to extradition between Parties for the criminal Criminal Procedure Code Articles 488-504 offences established in accordance with Articles 2 through 11 of this Law No. 10 193 from 03.12,2009 Convention, provided that they are punishable under the laws of both Parties \"On jurisdictional relations with foreign authorities in criminal matters". concerned by deprivation of liberty for a maximum period of at least one year, Criminal Procedure Code (unoficial translation) or by a more severe penalty.
- Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
- 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
- 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.
- 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.
- 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
- 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.  7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.  b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance  1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.	Criminal Procedure Code – Articles 505-508 Law No. 10 193 from 03.12.2009 "On jurisdictional relations with foreign authorities in criminal matters" Criminal Procedure Code (unoficial translation)
2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.	
3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.	
4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the	

PUDARECT CONVENTION	DOMESTIC LEGISLATION
BUDAPEST CONVENTION	DOMESTIC LEGISLATION
grounds on which the requested Party may refuse co-operation. The requested	
Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the	
request concerns an offence which it considers a fiscal offence.	
request concerns an orience which it considers a fiscal orience.	
5 Where, in accordance with the provisions of this chapter, the requested Party	
is permitted to make mutual assistance conditional upon the existence of dual	
criminality, that condition shall be deemed fulfilled, irrespective of whether its	
laws place the offence within the same category of offence or denominate the	
offence by the same terminology as the requesting Party, if the conduct	
underlying the offence for which assistance is sought is a criminal offence	
under its laws.	
Article 26 – Spontaneous information  1 A Party may, within the limits of its domestic law and without prior request,	Article 27 of Law No. 10 102 dated 02 12 2000
forward to another Party information obtained within the framework of its own	"On jurisdictional relations with foreign authorities in criminal matters"
investigations when it considers that the disclosure of such information might	On jurisdictional relations with foreign additionales in criminal matters
assist the receiving Party in initiating or carrying out investigations or	
proceedings concerning criminal offences established in accordance with this	
Convention or might lead to a request for co-operation by that Party under	
this chapter.	
2 Prior to providing such information, the providing Party may request that it	
be kept confidential or only used subject to conditions. If the receiving Party	
cannot comply with such request, it shall notify the providing Party, which	
shall then determine whether the information should nevertheless be	
provided. If the receiving Party accepts the information subject to the	
conditions, it shall be bound by them.	
Article 27 - Procedures pertaining to mutual assistance requests in	
the absence of applicable international agreements	
1 Where there is no mutual assistance treaty or arrangement on the basis of	
uniform or reciprocal legislation in force between the requesting and requested	
Parties, the provisions of paragraphs 2 through 9 of this article shall apply.	
The provisions of this article shall not apply where such treaty, arrangement	
or legislation exists, unless the Parties concerned agree to apply any or all of	
the remainder of this article in lieu thereof.	

#### **DOMESTIC LEGISLATION**

- 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
- b The central authorities shall communicate directly with each other;
- c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
- d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
- 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
- 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
- b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
- 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
- 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
- 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
- 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
inform the requesting Party, which shall then determine whether the request should nevertheless be executed.  9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.  b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).  c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.  d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requested Party.  e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use  1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.	Article 4, law No.8457, from 11.02.1999 "Classified Information "State Secret".
2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:  a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or  b not used for investigations or proceedings other than those stated in	

the request.

### **BUDAPEST CONVENTION DOMESTIC LEGISLATION** 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material. Article 29 - Expedited preservation of stored computer data A Party may request another Party to order or otherwise obtain the Law no. 9918 dated 19.05.2008 "On electronic communication" Article 101 expeditious preservation of data stored by means of a computer system, "Preservation and administration of data for the purpose of criminal located within the territory of that other Party and in respect of which the prosecution". requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. A request for preservation made under paragraph 1 shall specify: the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; the stored computer data to be preserved and its relationship to the offence: d any available information identifying the custodian of the stored computer data or the location of the computer system; the necessity of the preservation; and that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other

than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.  5	
requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data	
29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.  2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.  2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.  3 The request shall be responded to on an expedited basis where:  a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or  b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available  A Party may, without the authorisation of another Party:  a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or  b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.  2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data  The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications	

### **BUDAPEST CONVENTION DOMESTIC LEGISLATION** transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws. Article 35 - 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, According to the declaration made by Albania, the 24/7 Network point of contact seven-day-a-week basis, in order to ensure the provision of immediate designated by Albania is the: Cybecrime Unit, Albania State Police, Ministry of assistance for the purpose of investigations or proceedings concerning Interior criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; the collection of evidence, the provision of legal information, and locating of suspects. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network. Declaration contained in a Note verbale from the Permanent Representation of Article 42 - Reservations Albania, dated 19 June 2006, registered at the Secretariat General on 19 June By a written notification addressed to the Secretary General of the Council of 2006 - Or. Engl. Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it In accordance with Article 24, paragraph 7, of the Convention, Albania declares avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article that the name and address of the authorities responsible for making or receiving 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11 requests for extradition or provisional arrest in the absence of a treaty are: paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29 Ministry of Justice, Bulevardi Zog. I., Tirana paragraph 4, and Article 41, paragraph 1. No other reservation may be made. National Central Office of Interpol, Bulevardi Deshmoret e Kombit, Tirana.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Period covered: 19/6/2006
	The preceding statement concerns Article(s): 24
	Declaration contained in a Note verbale from the Permanent Representation of Albania, dated 19 June 2006, registered at the Secretariat General on 19 June 2006 - Or. Engl. In accordance with Article 27, paragraph 2, of the Convention, Albania declares that the name and address of the central authority responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution is: <b>Ministry of Justice</b> , Bulevardi Zog. I., Tirana Period covered: 19/6/2006
	Declaration contained in a Note verbale from the Permanent Representation of Albania, dated 10 October 2006, registered at the Secretariat General on 10 October 2006 - Or. Engl. The 24/7 Network point of contact designated by Albania is the: please contact <a href="mailto:alexander.seger@coe.int">alexander.seger@coe.int</a>